Развернуть gitlab v16.8.1 в kubernetes кластере

Чтобы развернуть раннеров использовал helm и helmfile.

Чарт гитлаба (версия чарта 7.8.1; версия гитлаба 16.8.1

<https://gitlab.com/gitlab-org/charts/gitlab/-/tree/v7.8.1?ref_type=tags>

В файле deps.yaml указаны зависимости

Развернул postgres в кубе, для этого развернул db operator. С помощью него сделал отдельную бд для гитлаба. Уменьшил обьем pvc postgres.

Чарт db operator

<https://github.com/db-operator/charts/tree/main/charts/db-operator>

Чарт postgres

<https://github.com/bitnami/charts/tree/main/bitnami/postgresql>

Далее развернул redis. Убрал pvc.

Чарт redis

<https://github.com/bitnami/charts/tree/main/bitnami/redis>

Написал манифест бд для гитлаба

Затем развернул гитлаб, предварительно отключив установку других зависимостей и настроив ingress, psql и редис. Но для гитлаба были необходимы minio, gitaly и shared secrets

pvc создаваемый gitaly весил 50гб, на время тестирования уменьшил до 5

minio уже развернут, но не настроен, также устанавливал через зависимости

После изменений гитлаб развернулся, но все ингрессы использовали nginx, а не traefic.

Настроил ingressclass (указал global.ingress.class: traefic)

Зааплаил изменения, но поды не деплоились, так как не видели секрет с паролем для редиса.

Поставил reflector

Ссылка на чарт:<https://github.com/emberstack/kubernetes-reflector>

Задал для редиса

secretAnnotations:

reflector.v1.k8s.emberstack.com/reflection-allowed: "true"

reflector.v1.k8s.emberstack.com/reflection-auto-enabled: "true"

reflector.v1.k8s.emberstack.com/reflection-allowed-namespaces: "gitlab"

Чтобы секрет с паролем редиса копировался в неймспейс гитлаба

Не смотря на то что секрет в неймспейсе появился, поды все равно не деплоились, название секрета было указанно gitlab-redis-secret, а не redis

Заменил название секрета в global.redis.auth, но поды все равно искали секрет с названием gitlab-redis-secret. Далее заменил аналогичные значения в redis.auth, также безрезультатно. Попытался задать название файла с секретом для всех зависимостей, но даже так поды искали не тот секрет

Задал пароль для redis

Обновил global.redis.auth

<https://docs.gitlab.com/charts/advanced/external-redis/>

Настроил сертификаты cert-manager

<https://docs.gitlab.com/charts/charts/globals#globalingressconfigurecertmanager>

minio.enabled устарел, поэтому использую global.minio.enabled и minio.ingress

Изменил версию гитлаба на Community Edition

Настроил баккиты в минио

Добавил юзера gitlab с доступом к этим баккитам

Написал манифест для секрета с кредами

Выбрал секрет с кредами для гитлаба

registry и toolbox задаются отдельно, они задеплоились без проблем

webservice и sidekiq пытаются прочитать локальный файл /etc/gitlab/objectstorage/artifacts

Задал global.appConfig.object\_store.enabled: true, получил такую же ошибку

<https://docs.gitlab.com/charts/advanced/external-object-storage/>

Задал баккиты и секрет

<https://gitlab.com/gitlab-org/charts/gitlab/blob/master/examples/values-external-objectstorage.yaml>

Секреты объединил в 1 манифест

Секрет для rails:

<https://gitlab.com/gitlab-org/charts/gitlab/-/blob/master/examples/objectstorage/rails.s3.yaml>

Секрет для registry:

<https://gitlab.com/gitlab-org/charts/gitlab/-/blob/master/examples/objectstorage/registry.s3.yaml>

Поды получали данный s3

Увеличил память до 16гб

Увеличил количество ядер до 16

Увеличил failureTreshold до 10

Зашел за админа и создал пользователя, за этого пользователя сделал репу. Далее эту репу удалил. Через какое-то время при создании репы стал получать ошибку 500.

Создать репу смог, видимо сервер был загружен при прошлой попытке

Смог запулить репу через https

Добавил ssh ключ, но при git pull получал ввод пароля

Для ускорения теперь ключи берутся из бд, а не файла authorized\_keys

<https://docs.gitlab.com/ee/administration/operations/fast_ssh_key_lookup.html>

Проверил бд, мой ключ добавился в бд в таблицу keys

Развернул traefik (до этого он был развернут дефолтно)

<https://github.com/traefik/traefik-helm-chart/blob/master/traefik/values.yaml>

Открыл 22 порт и сделал редирект с 80 на 443

После того как открыл порт смог клонировать репу через ssh

Настроил tls для минио, был 1 сертификат и для s3, и для консоли; сделал 2 сертификата

Добавил секрет для toolbox

<https://docs.gitlab.com/charts/advanced/external-object-storage/#backups-storage-example>

Попробовал сделать бекап

<https://docs.gitlab.com/charts/backup-restore/backup.html>

Версия pg\_dump 15.1, версия psql 16.1, не получилось забекапить дб

k exec -it gitlab-toolbox-7c78b6966d-smcn2 -- backup-utility

Получил ошибку

ERROR: S3 error: 400 (IllegalLocationConstraintException): The af-south-1 location constraint is incompatible for the region specific endpoint this request was sent to.

command terminated with exit code 11

Проверил работает ли minio с помощью rclone

Сделал конфиг и rclone lsd

Получил бакиты

Заменил s3tool

k exec -it gitlab-toolbox-7c78b6966d-smcn2 -- backup-utility --s3tool awscli

upload failed: srv/gitlab/tmp/backup\_tars/1707234444\_2024\_02\_06\_16.8.1\_gitlab\_backup.tar to s3://gitlab-backup-storage/1707234444\_2024\_02\_06\_16.8.1\_gitlab\_backup.tar Unable to locate credentials

command terminated with exit code 1

Думаю пока что можно делать бекапы в лонгхорне

Проверил работу бекапов через лонгхорн

kubectl port-forward -n longhorn-system services/longhorn-frontend 8080:80

Сделал снепшоты для gitaly и postgresql

Удалил репу чтобы проверить gitaly и ключ чтобы проверить psql

kubectl edit <Kind> -n <namespace <deployment/statefulset name>

Поставил количество реплик для gitaly и psql на 0

Зашел на localhost:8080/, зашел в volumes и выбрал для pvc gitaly и postgresql attach in maintenance, восстановил снапшот

Поставил количество реплик для gitaly и psql на 1

И репа и ключ были восстановлены

Проверил lfs

В <settings -> general -> Visibility, project features, permissions> lfs включен по дефолту.

Добавил в репу большой файл

git-lfs track ..., запушил, файл отображается как lfs

lfs файлы в баките gitlab-lfs в minio

Проверил registry

docker login registry.gitlab.k8s.eterfund.ru

docker build -t registry.gitlab.k8s.eterfund.ru/jacklull/testproject .

docker push registry.gitlab.k8s.eterfund.ru/jacklull/testproject

Получил ошибку

error parsing HTTP 403 response body: unexpected end of JSON input: ""

Но в баките gitlab-registry находятся файлы на 9Кб, следовательно registry видит minio, но не может полностью загрузить туда образ